

REMARKS

Favorable reconsideration of this application, as presently amended and in light of the following discussion, is respectfully requested.

In the present Application, Claims 23-29 are pending. The present Amendment cancels Claims 1-22 without prejudice or disclaimer, and adds new Claims 23-29 without introducing any new matter.

In the Official Action, Claims 1-4, 6, 14 and 22 were rejected under 35 U.S.C. § 103(a) as being unpatentable over Ono et al. (U.S. Patent No. 6,496,930; hereinafter “Ono”) in view of Hall (U.S. Patent No. 5,126,728). Claims 7-11 and 15-20 were rejected under 35 U.S.C. § 103(a) as being unpatentable over Ono in view of Hall, in further view of Yoshizawa (U.S. Patent No. 6,928,166). Claims 5, 12-13 and 21 were rejected under 35 U.S.C. § 103(a) as being unpatentable over Ono in view of Hall, Yoshizawa and further in view of Tanaka et al. (U.S. Patent No. 6,208,376; hereinafter “Tanaka”).

First, Applicants wish to thank Examiners Pan and Truong for the courtesy of an interview granted to Applicants’ representative Nikolaus P. Schibli, Reg. No. 56,994, on November 6, 2008, at which time the outstanding issues in this case were discussed. During the interview the pending rejections were discussed, and it was further concluded that new claims will be presented that are better directed to the generic embodiment of Fig. 4. The Examiner indicated that he would reconsider the outstanding grounds for rejection upon formal submission of a response.

In response to the results of the Interview, Claims 1-22 cancelled and new Claims 23-39 are presented. New independent Claim 23 is directed to a mobile communication terminal device, including a detection unit and an announcing unit. These features find non-limiting support in Applicants’ disclosure as originally filed, for example in Fig. 4, Steps S2 and S3, and in the specification at p. 15, 11-25, and in Fig. 1, reference numerals 4 and 5. No new

matter has been added. New dependent Claim 24 depends upon independent Claim 23, and recites features related to an user interface operable by an user, and finds non limiting support in Fig. 5, and at p. 16, 15-20. New dependent Claim 25 depends upon independent Claim 23, and recites features related to a data security setting unit, finding non-limiting support in Fig. 1, reference numeral 7, Fig. 6, and at p. 17, ll. 8-20. New dependent Claim 26 depends upon independent Claim 23, and recites feature related to a threshold security level, finding non-limiting support in Fig. 7, and in the specification at p. 18, ll. 2-25. New dependent Claim 27 depends upon Claim 25 and finds non-limiting support at p. 18, ll. 18-20. New dependent Claim 28 depends upon Claim 27 and finds non-limiting support at p. 13, ll. 15-16. New dependent Claim 29 depends upon independent Claim 23, and recites features directed to more than one network. These features find non-limiting support in the specification at p. 20, ll. 7-10. No new matter has been added.

New Claims 33-39 recite features that are analogous to the features of new Claims 23-29, but directed to a method. New Claims 30-32 are directed to a server, and support for these claims can be found at least in original Claims 7-9.

In response to the rejection of Claim 1 under 35 U.S.C. § 103(a), in light of the presentation of new claims, Applicants respectfully request reconsideration of this rejection and traverse the rejection, as discussed next.

Briefly summarizing, new Claim 23 is directed to a mobile communication terminal device configured to perform encrypted communication with a communication system over a wireless connection. The terminal device includes ***a detection unit configured to establish a communication activation procedure with the communication system, and configured to detect a security level that is used during the communication activation procedure*** with the communication system; and an announcing unit configured to inform a user of the mobile

communication terminal device about a strength of encryption of the detected security level from the communication activation procedure.

Turning now to the applied references, Ono is directed to a client apparatus 2 that generates data for producing a message input form which urges a user to enter a message, and to enter data to specify a data conversion type for secret communication of the message to a server 4. (Ono, Abstract, Fig. 1.) Ono explains that the client apparatus can specify whether to encrypt the message, and can decide which encryption method should be used, based on his own specification. (Ono, col. 3, ll. 17-22.) Moreover, Ono's Fig. 7 shows a flowchart how the message is created and sent. (Ono, Fig. 7, col. 12, ll. 17-18.) Ono explains that the user will see a message input form on his screen of the terminal apparatus 2. (Ono, Fig. 7, step S203.) The user can thereby enter a "encryption variable," specifying an encryption method, for example RSA, and thereafter, the message is sent using the specified encryption method. (Ono, col. 12, ll. 28-40.) However, Ono fails to teach all the features of Applicants' Claim 23. In particular, Claim 23 requires

a detection unit configured to establish a communication activation procedure with the communication system, and configured to detect a security level that is used during the communication activation procedure

(Claim 23, portions omitted.) Ono merely explains that the user can pick his encryption method, and that the message is then sent with the chosen encryption method, as discussed *supra*. There is no communication activation procedure in Ono that is used to detect an available security level, as required by new independent Claim 23. In addition, Ono also fails to teach an announcing unit configured to inform a user about a strength of encryption of the detected security level *from the communication activation procedure*. (Claim 23, portions omitted, emphasis added.) In Ono, a user merely enters his choice of encryption.

The reference Hall, used by the pending Office Action to form a 35 U.S.C. § 103(a) rejection, fails to remedy the deficiencies of Ono, even if we assume that the combination is

proper. Hall is directed to a data processing security device 103 having a microcontroller 107 that is configured to insert data labels into a data stream, or to detect data labels of a data stream. (Hall, Abstract, Fig. 3.) Hall further explains that the device can detect labels within the data protocol field that indicates a security level, and can allow it to pass, or block it. (Hall, col. 11, ll. 40-46.) But Hall fails to remedy the deficiencies of Ono, and also fails to teach a detection unit to establish a communication activation procedure with the communication system, and configured to detect a security level that is used during the communication activation procedure as required by Claim 23. As explained in Hall, the device 103 is merely configured to observe passing data traffic to block it or let it pass.

Therefore, even if the combination of Ono and Hall is assumed to be proper, the cited passages of the combination fails to teach every element of Applicants' new Claim 23. Accordingly, Applicants respectfully traverse, and request reconsideration of this rejection based on these references.

Moreover, new independent Claim 30 is directed to a server configured to perform encrypted communication with a mobile user terminal over a wireless connection. The server includes, *inter alia*: a detection unit configured to establish a communication activation procedure with the mobile user terminal, and configured to detect a security level that is used during the communication activation procedure with the mobile user terminal. As discussed above, the applied references Ono and Hall fail to teach such a feature, even if the combination is assumed to be proper. In addition, the reference Yoshizawa fails to remedy the deficiencies of Ono and/or Hall. Yoshizawa is directed to a system that allows flexible security level switching, by using a password management section 17 and a password selecting section 18, where the most suitable password can be selected in dependence of a user event 21. (Yoshizawa, Abstract, Fig. 1.) However, Yoshizawa is silent on the detection unit configured to establish a communication activation procedure with the communication

system, and configured to detect a security level that is used during the communication activation procedure, as required by Applicants' independent Claim 30. Yoshizawa merely explains that a request for connection can be made between a device A and B, to ascertain a secure authentication method by using passwords for different situations. (Yoshizawa, col. 5, ll. 58-65, col. 6, ll. 6-28.) Yoshizawa is entirely silent on anything related to a security level related to encryption, but only authentication. Therefore, Applicants believe that the features of new independent Claim 30 are patentably distinct over the applied references Ono, Hall and Yoshizawa, taken in any proper combination.

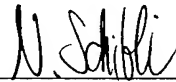
Independent Claims 33 recites features that are analogous to the features recited in independent Claim 23, but directed to a method. Accordingly, for the reasons stated above for the patentability of Claim 23, Applicants respectfully submit that the rejections of Claim 33, and the rejections of all associated dependent claims, are also believed to be overcome in view of the arguments regarding independent Claim 23.

Consequently, in view of the present amendment, no further issues are believed to be outstanding in the present application, and the present application is believed to be in condition for formal Allowance. A Notice of Allowance for Claims 23-39 is earnestly solicited.

Should the Examiner deem that any further action is necessary to place this application in even better form for allowance, the Examiner is encouraged to contact Applicants' undersigned representative at the below listed telephone number.

Respectfully submitted,

OBLON, SPIVAK, McCLELLAND,
MAIER & NEUSTADT, P.C.



Bradley D. Lytle
Attorney of Record
Registration No. 40,073

Customer Number
22850

Tel: (703) 413-3000
Fax: (703) 413 -2220
(OSMMN 03/06)

Nikolaus P. Schibli
Registered Patent Agent
Registration No. 56,994